Japanese Patent Laid-open No. HEI 8-322034 A
Publication date : Dec. 3, 1996
Applicant : Matsushita Denki Sangyo K.K.
Title : SCRAMBLING CONTROL METHOD

[Conventional art] In order to keep the contents of communication secret in satellite communication, the video/sound signal is transmitted after being scrambled. Thus, only a decoder having viewing/listening rights can view/listen to the communication by descrambling the same. Between analog video signals and digital video signals, digital video signals can be transmitted effectively in a small frequency range by the development of image coding techniques.

[0003] Fig. 3 is a schematic diagram of the digital video signal based on the MPEG (Moving Picture Experts Group) standards ISO 11172 and 13818. The digital video signal in this schematic diagram is a layered structure including six layers, that is, a video sequence layer, a GOP (Group Of Picture) layer, a picture layer, a slice layer, a macro block layer, and a block layer. Among these six layers, the top three layers of the layered structure, namely, the video sequence layer, the GOP layer, and the picture layer are shown.

[0004] The video sequence layer includes at least one GOP layer. The sequence header before each GOP layer has been omitted in the diagram. The GOP layer, which includes multiple pictures from I pictures, P pictures, and B pictures as image types corresponding to a predictive coding method, usually includes 15 or 12 pictures. At the head is set an I picture, which becomes the reference of the standard. The I picture is a picture for completely encoding within the picture. The P picture is a picture

that carries out prediction from the previous picture(s). The B picture is a picture that carries out prediction from the previous and following pictures. 1 second of video images includes 30 pictures. 1 GOP is the smallest unit for decompressing a video signal and the first complete video image can be displayed by all of the data from the beginning to the end of the GOP being aligned. A video signal image cannot be displayed by only data partway through the GOP.

[0005] Fig. 4 is a schematic diagram of the transmission method for the digital video signal based on the MPEG mentioned above. This transmission method has been standardized by international standards (ISO 13818-1) as MPEG systems. Each GOP unit in the GOP layer of Fig. 3 in the digital video signal is transmitted by multiple packets called transport packets (1) to (n) (hereinafter, "TS packet") having 184 bytes. Each TS packet is a fixed-length packet with a 4-byte header and a total of 188 bytes.

[0006] A conventional scrambling control method will be explained with reference to the timing chart in Fig. 2. In Fig. 2, line a indicates time. Lines b, c, d, e, and f are common times. Line b indicates a state when a digital signal of GOP units is transmitted by being divided into TS packet units. For ease of explanation, a number has been allocated to each GOP and TS packet. A part of GOP0, GOP1, GOP2, GOP3 and a part of GOP4 are shown. The state when the three GOPs of GOP1, GOP2, and GOP3 are transmitted by being divided into n TS packets including TS1 to TSn is shown. TS1 to TSn, the TS packets of GOP2, are transmitted in order between the times t4 and t6. TS1 to TSn, the TS packets of GOP3 are transmitted in order from time t6.

[0007] Line c indicates a state on the transmission side

when a digital signal is scrambled while updating scramble keys Ks1, Ks2, ... for each updating period T1. In an updating period T1 from the times t1 to t5, the TS packet to be transmitted is scrambled by the scramble key Ks1 and between the times t5 and t7 the TS packet to be transmitted is scrambled by the scramble key Ks2.

[0008] The updating period T1 of the scramble key is constant and is a short period of a number of seconds. There is no relationship between the timing for updating the scramble key and the GOP. The data transmitted by the first TS packet after updating of the scramble key in most situations becomes data partway through the GOP. In Fig. 2, the state of updating the scramble key from Ks1 to Ks2 in the time t5, which is partway through GOP2 between the times t4 and t6, is shown.

[0009] Line d indicates a timing of distributing the scramble key from the transmission side to the reception side. The transmission side, in parallel with a scrambling process like the one mentioned above, distributes the scramble key Ks2 in advance for a decoder allowing viewing/listening in the time t3, which is between the scrambling of the TS packet to be transmitted between the times t1 and t5, by the scramble key Ks1.

[0010] Line e received this channel a long while ago on the reception side and indicates a state of the decoder of the reception side in the steady state. The decoder in the steady state, by using the scramble key that is distributed in advance from the transmission side, descrambles the TS packets received between the times t1 and t5, in other words, the TS packets of a part of GOP0, the TS packets of GOP1, and the TS packets of a part of GOP2. In parallel with the descrambling process, the scramble key Ks2 is received in advance at the time t3 and the TS packets

received between the times t5 and t7, in other words, the TS packets of a part of GOP2, the TS packets of GOP3, and the Ts packets of GOP4, are descrambled by Ks2.

Accordingly, because all of the TS packets of GOP1 are descrambled by scramble key Ks1, all of the TS packets of GOP2 are descrambled by descramble keys Ks1 and Ks2, and all of the packets of GOP3 are descrambled by the scramble key Ks2, the complete video images of GOP1, GOP2, and GOP3 can be displayed by decompressing the complete video images.

[0011] When the decoder is not in the steady state, as indicated by line f, a decoder that starts reception of a channel from the time t2 by turning on the power of the decoder or changing of the channel will be explained. Directly after reception of the channel has started, the reception decoder does not have the scramble key Ks1. Therefore, the TS packets to be received cannot be descrambled between the times t2 and t5. Therefore, the video images cannot be decompressed and displayed for the GOPs until time t5.

[0012] Even if reception of the channel starts from the time t2, the scramble key Ks2 can only be received at the time t3. Therefore, descrambling of the packet is possible at the time t5. The TS packets descrambled between the times t5 and t6 are TS packets from partway through GOP2. Therefore, the video image of GOP2 cannot be decompressed. The start of decompression of the complete video image is from GOP3, which starts descrambling from the head data in the time t6.

[0013] Therefore, from the beginning of reception to when scrambling can begin is the time t2 to t5 and the time T2, which is the time while descrambling can be done but image display is not possible, in other words, the time t5

to t6. The waiting time from when reception starts until image display is the time t5 to t6. The maximum time of T2 is the time of 1 GOP. Therefore, when 1 GOP includes 15 pictures, it becomes 0.5 seconds.

[0014]

[Problem to be Solved by the Invention]

In the conventional scrambling method explained above, as indicated by the line f, in the waiting time from when reception starts until image display, at a TS packet level, there is a time T2 in which scrambling can be performed, but image display is not possible. Therefore, there is a problem that the waiting time becomes much longer.

[0015] In consideration of the above problem, an object of the present invention, at the TS packet level, is to eliminate the time in which descrambling can be performed but image display is not possible in the waiting time needed from the start of reception by changing the channel until image display, and to be able to decrease the waiting time.

[0016]

[Means to Solve the Problems]

The present invention solves the problem by a control method in which GOP units based on MPEG, which is an international standard in decoding of moving pictures, are divided into multiple transport packets, transport packets are transported after each has been scrambled by a scramble key, and the scramble keys are updated from the time of transmitting a transport packet including head data of GOP units. In this situation, at the reception side, by the transmission side distributing the scramble keys mentioned above to the reception side in advance, when reception starts partway through the GOP units, by scramble keys distributed in advance from the transmission side,

descrambling from the transport packet including head data of a next GOP unit can be performed and decompression of the corresponding GOP unit is possible.

[0017]

[Operation] By the control method mentioned above, the present invention can update the scramble key from the transmission time of the transport packet including the head data of GOP units. Therefore, at the reception side, when reception starts partway through GOP units transmitted from the transmission side, descrambling can be performed from the head data of the transport packet of the next GOP unit. Therefore, decompression of a complete video signal can start by the decompression of this GOP unit, and the waiting time from the start of reception can be decreased.

[Fig. 1] A timing chart of a scrambling control method according to an embodiment of the present invention.

[Fig. 2] A timing chart of a conventional scrambling control method.

Fig. 1, 2

(Time axis)

(GOP and TS packet)

(Used scramble key)

(Scramble key distribution)

(Steady state decoder)

(Reception starting decoder)

TS packets transmitted during this period are scrambled by Ks1

TS packets transmitted during this period are scrambled by Ks2

Distribution of Ks2

Distribution of Ks3

TS packets received during this period are descrambled by Ks1

TS packets received during this period are descrambled by Ks2

Reception of Ks2

Reception of Ks3

Decompression of GOP0

Decompression of GOP1

Decompression of GOP2

Decompression of GOP3

Decompression of GOP4

Descrambling of TS packets is not possible

Start of reception

(図２　GOP2は復元不可)

Decompression of GOP2 is not possible

Waiting time